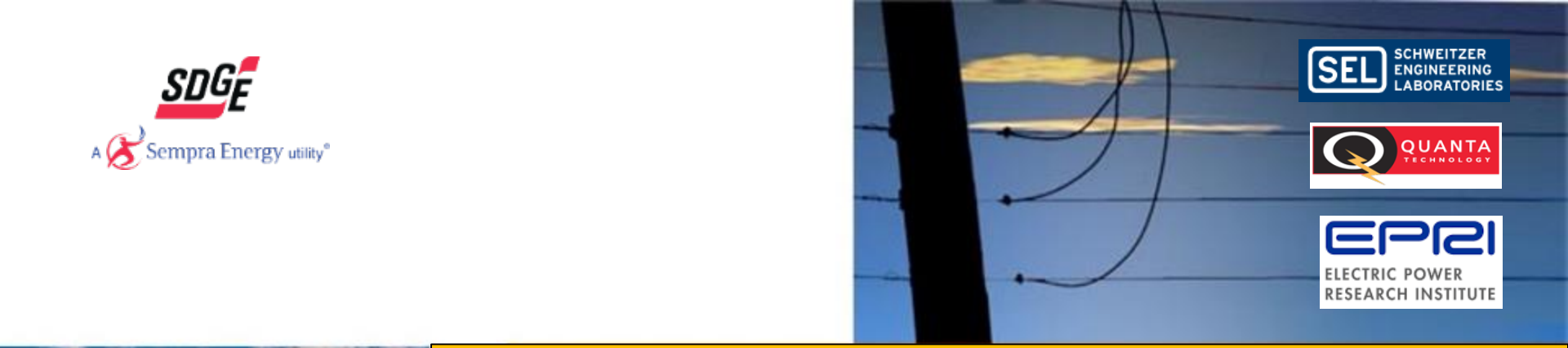


GPS spoofing tests of PMU's used for mission-critical synchrophasor applications

Tariq Raman, *San Diego Gas & Electric®*
Mike Bryson, Schweitzer Engineering Laboratories, Inc.
Solveig Ward , Quanta Technology, LLC
Gerardo Trevino, EPRI

Presented at NASPI, October 30, 2019
Richmond, VA

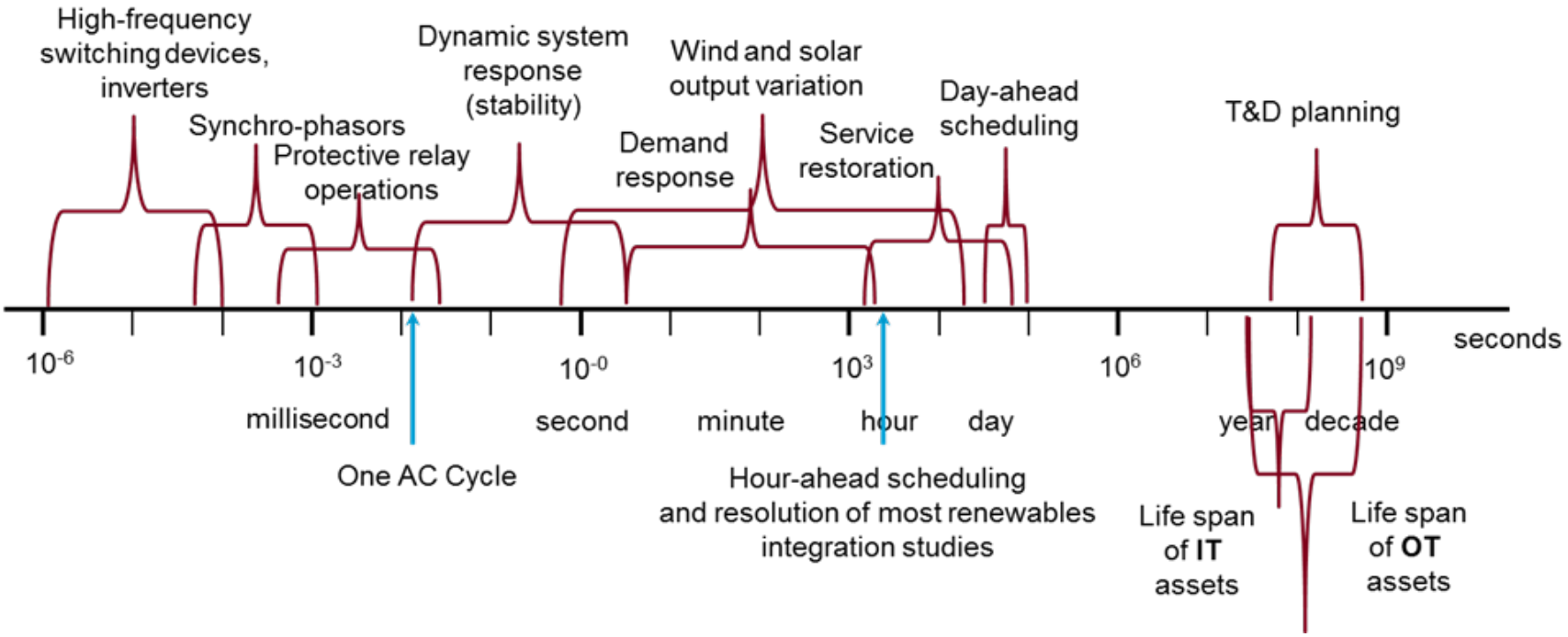
© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Introduction

- Integrated time synchronized operations lead to improved safety, flexibility, and reliability of the electric supply.
- Highly accurate time sources are required for wide area applications.
- Applications based on synchrophasor measurements are using time stamped measurements from various points in the power system.
- These measurements are time aligned by the application that will then indicate the state of the power system which is to be used for operational actions.
- Advances in power system monitoring, control and protection are made by deployment of intelligent field devices that collect data and communicate this data to typically centralized applications that evaluate the data from the power system and executes control or protection actions.
- All these applications rely on accurate time synchronization of field devices.

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Utility Data Spans a Wide Time Scale



© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

GPS spoofing

- Many incidents of GPS spoofing are being reported on a daily basis, but mostly focuses on location errors and not time data errors.
- For the power system applications examined by SDG&E, location is not important, but time data is.
- The effect from erroneous time data on applications relying on time data was tested and evaluated.
- Misoperation of current differential relays were observed.
- PMU phasor drift was observed but the resulting effect on the synchrophasor applications was not evaluated in detail.

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Applications

- The applications planned by SDG&E include:
  - Wide-Area Situational Awareness
  - Wide-Area Data Analysis
  - Protection, Control and RAS functions
  - Wide-area Back-up Fault Protection
  - Wide-area Voltage Swing Protection
  - Synchrophasor Island-Balancing Remedial Action Scheme
  - Synchrophasor-assisted Black Start
  - Fallen conductor detection
- None of these applications will operate properly if erroneous time stamps are used
- Erroneous time stamps must be detected and mitigated for proper application performance.

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test plan

- SDG&E performed a vulnerability assessment of time synchronization equipment deployed to attacks that could impact synchronized operations.
  - Objective: Understand effects on equipment and risks for applications from GPS cyber attacks.
  - Future work will need to focus on mitigation.
- Leveraging SDG&Es Integrated Test Facility (ITF) Lab, the project team set up a real time hardware in the loop (HiL) test setup.
- The time data was manipulated using a real time GNSS simulator with custom scripts designed to exploit the GPS receivers' vulnerabilities and to allow for the impact on power system applications under test to be observed.

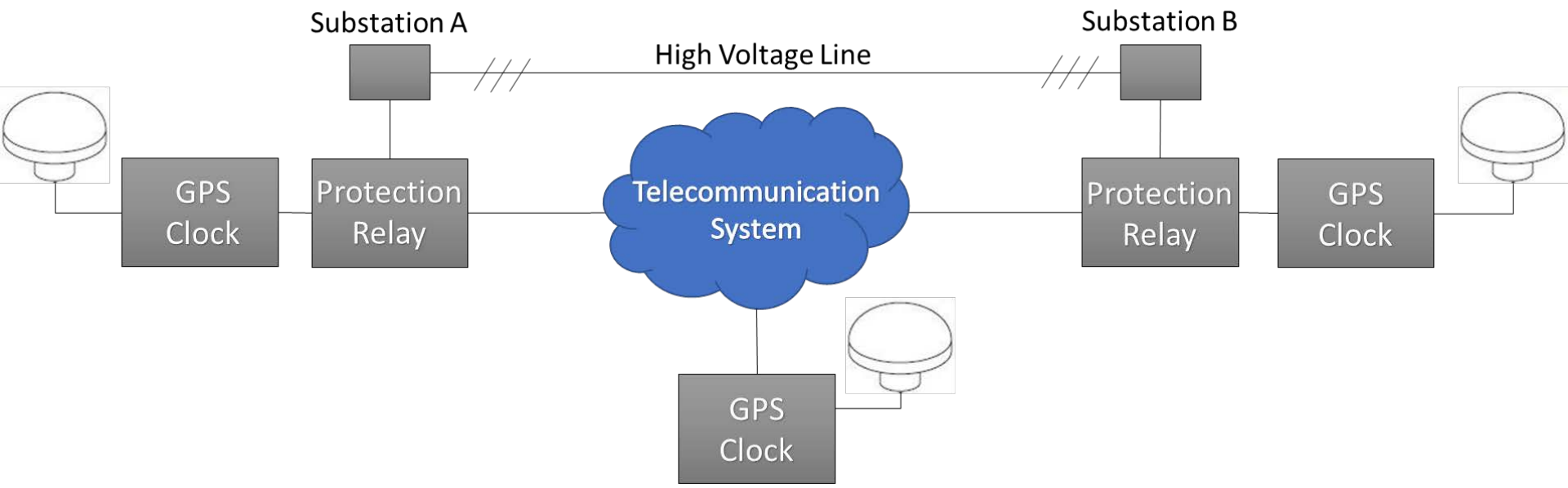
© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test requirements and test setup

- To identify timing vulnerability effects, individual relays with PMU functions were tested using known attack vectors emanating from GPS sources (i.e. spoofing).
- Testing was made with an RTDS power system model reflecting a real power system.
- For synchrophasor testing, steady state test conditions were used.
- Various combinations of GPS source manipulations were conducted.
- The tests were performed by introducing a time drift of one GPS clock, while keeping another GPS clock as a reference source.
- The clocks were supplying GPS to the devices under test in various combinations and for various configurations.

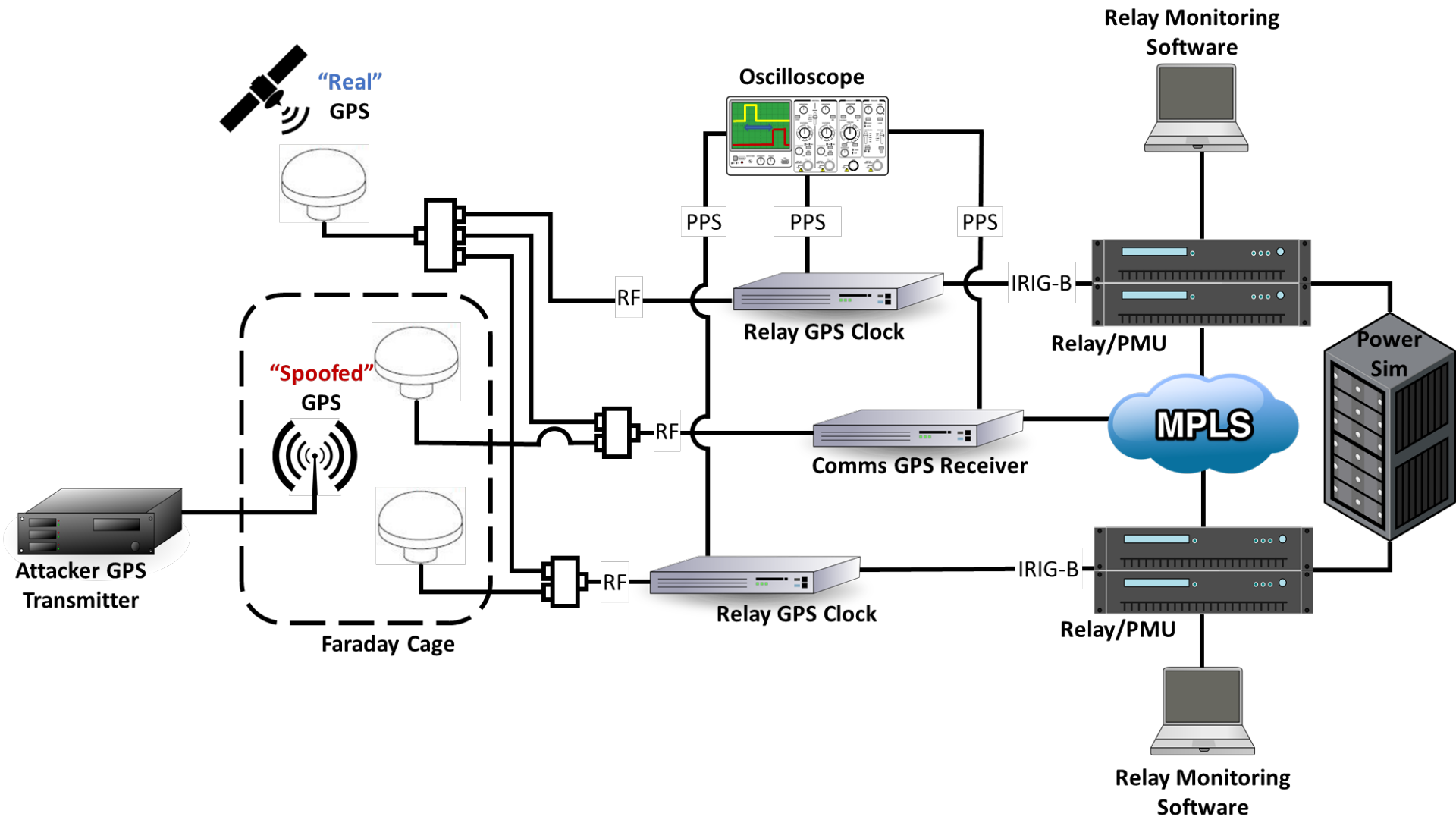
© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test setup



© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test setup (cont.)



© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test equipment (cont.)

- Synchrowave Central
  - To illustrate the phase shift of synchrophasor measurements

- Equipment under test
  - Relays providing synchrophasor data

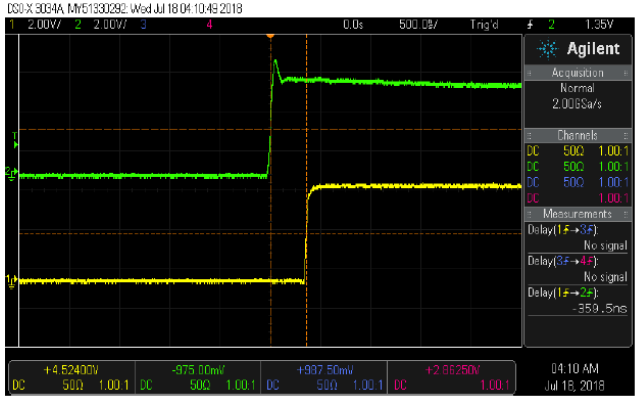
- GPS clocks

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test equipment

- Frequency counter
  - Measures time difference between GPS receivers

- Oscilloscope
  - Shows the offset between the clock signals

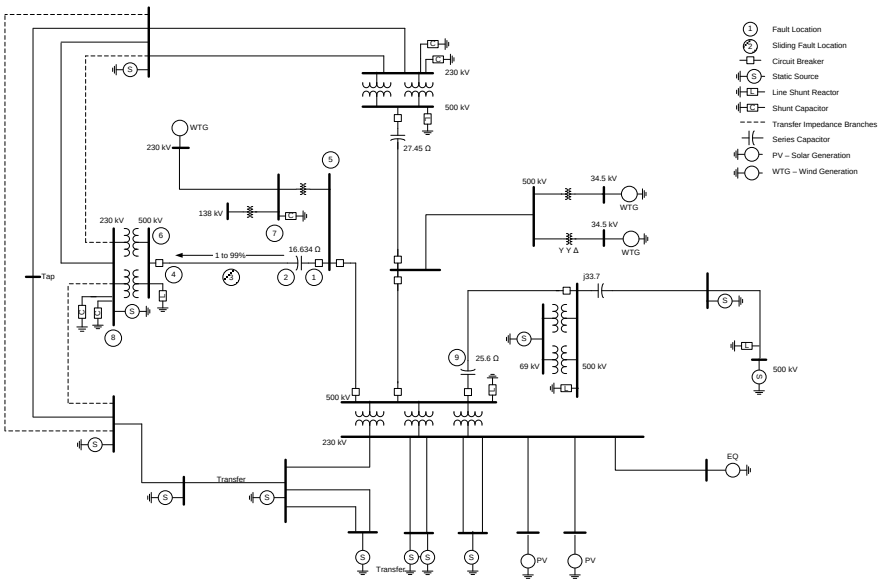


- GPS and GLONASS simulator
  - Produces both nominal and attack GPS signals

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test setup (cont.)

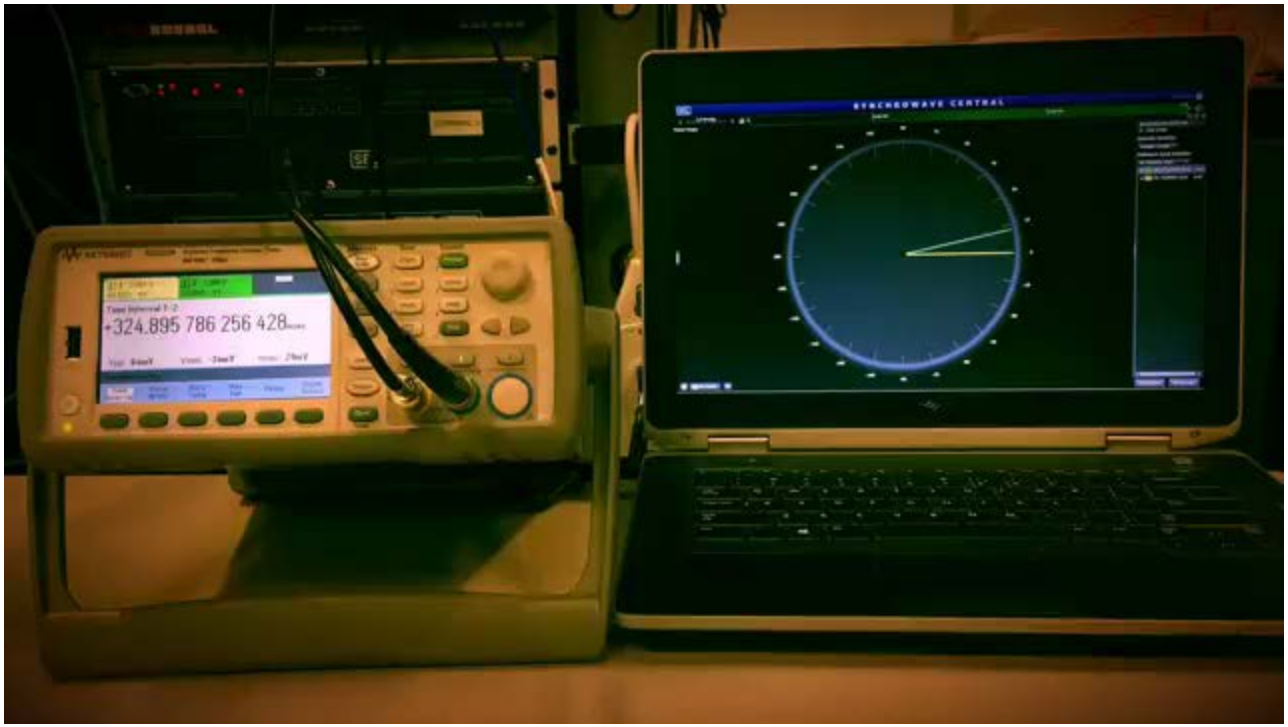
- RTDS® real-time fault simulation
  - For synchrophasor testing, steady state condition was simulated



© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Test results

- The tests included current differential relays, and the misoperations are documented in the video.
- The effect on the synchrophasor applications were not directly tested but only observed in the form of phase shifts of the synchrophasors that would impact all applications if not detected and mitigated.



© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Conclusions

- The project identified vulnerabilities resulting from time synchronization spoofing which will be greatly detrimental to all synchrophasor applications and the project team believes there is great value of making the synchrophasor community aware of this risk.
- While the project identified vulnerabilities of time synchronized applications, future work is needed to define and research detection and mitigation methods.
- GPS clock designs are continuously improving to address spoofing attacks; however, it is suggested that the synchrophasor applications also need to consider the very real risk of spoofing and implement methods to detect and mitigate spoofing attacks.

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Conclusions (cont.)

- GPS clock devices used in applications were vulnerable to GPS cyber-attacks.
- Equipment connected to vulnerable GPS clocks do not have logic to detect slow timing drifts. As a result they provide incorrect time data
- Applications that rely on GPS can be significantly degraded if proper mitigations are not in place
- More research/testing should be conducted at the system level (vs device level)
- More research/testing should be conducted to incorporate active protection technologies to understand the efficacy to protect against GPS cyber attacks

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Recommendations

For all the tested applications, it is suggested that regular industry methodologies are followed including **detection**, **protection**, **identification**, **response** and **recovery**.

- From a cyber security perspective, it is not possible to protect what you do not own. Utilities do not own the RF spectrum therefore it is not possible to **protect** the GPS receivers from RF attacks
- How this is accomplished will vary depending on what devices (clocks, network time) are installed in the field and on the intelligence in the receiving application.
- There are technologies commercially available that allow for the detection and direction finding of aberrant GPS signals.
- In order to increase the resilience of applications to these attacks new designs should incorporate timing backup systems or redundant mechanisms to be able to properly operate in the presence of an event.
- During testing, some equipment to some extent was able to **identify** time errors that caused asymmetry in the communications for these applications. PMUs did not. Monitoring of GPS receivers and other equipment is recommended.
- Even when relays, also performing PMU functions, detected timing errors, it did not invalidate the PMU function.

It was of great concern that the data from the relays/PMUs was not useful in indicating that there was a time source error.

- It is recommended to consider installing GPS jamming and spoofing detection technologies to increase the level of situational awareness related to these types of attacks

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.

Thank you!

© 2019 San Diego Gas & Electric Company. All copyright and trademark rights reserved.